

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number Q102939
Mail Stop AF Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450	Application Number 10/762,364	Filed January 23, 2004
	First Named Inventor Roger MAITLAND	
	Art Unit 2434	Examiner Ellen C. TRAN
<p style="text-align: center;">WASHINGTON OFFICE 23373 CUSTOMER NUMBER</p>		
<p>Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.</p> <p>This request is being filed with a notice of appeal</p> <p>The review is requested for the reasons(s) stated on the attached sheet(s). Note: No more than five (5) pages may be provided.</p> <p><input checked="" type="checkbox"/> I am an attorney or agent of record.</p> <p>Registration number <u>28,703</u></p> <p style="text-align: right;"><u>/DJCushing/</u> Signature</p> <p style="text-align: right;"><u>David J. Cushing</u> Typed or printed name</p> <p style="text-align: right;"><u>(202) 293-7060</u> Telephone number</p> <p style="text-align: right;"><u>August 4, 2009</u> Date</p>		

PATENT APPLICATION
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Docket No: Q102939

Roger MAITLAND

Appln. No.: 10/762,364

Group Art Unit: 2434

Confirmation No.: 4471

Examiner: TRAN, ELLEN C

Filed: January 23, 2004

For: METHODS AND APPARATUS FOR PARALLEL IMPLEMENTATIONS OF TABLE
LOOK-UPS AND CIPHERING

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MAIL STOP AF - PATENTS

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Sir:

Pursuant to the Pre-Appeal Brief Conference Pilot Program, and further to the Examiner's Final Office Action dated March 4, 2009, Applicant files this Pre-Appeal Brief Request for Review. This Request is also accompanied by the filing of a Notice of Appeal.

Claims 1-79 are pending, of which claims 1, 12, 21, 35, 49-51, 55, 64, and 73-76 are independent. Claims 74-79 are rejected as unpatentable over Kim et al (WO 03/050784) in view of Luyster (USP 6,751,319). Claims 1, 2, 5, 6, 11-13, 16, 21-28, 30, 31, 33-42, 44, 45, 47-73 and 77-79 are rejected as unpatentable over Kim et al in view of Luyster and further in view of 3GPP TS 35.202 v3.1.1 Release 1999 (3GPP). Claims 3, 4, 7-10, 14, 15, 17-20, 29, 32, 34, 43 and 46 are rejected as unpatentable over Kim et al in view of Luyster and 3GPP, and further in view of Weybrew et al (USP 6,931,511).

Claims 74-76 –

Claims 74-76 are directed to the simultaneous use of different parts of a signal to address one or more lookup tables. The examiner acknowledges that Kim does not teach the use of lookup tables. The examiner cites Luyster for its teaching of look-up tables, but the novelty in claim 74 is not simply the use of a lookup table but the parallel use of different parts of a single input signal to address different lookup tables or different parts of a lookup table. This novelty is stated at lines 22-27 of page 2 of the present application as filed.

At page 6 of the final Office action, the examiner reads the upper 16 bits and lower 16 bits of the 32-bit input in Kim as the claimed plurality of inputs, but this is an unreasonable reading of the claim language and Kim *et al.* There is only one input in Kim *et al.*, a 32-bit input. The upper and lower sets of bits are different parts of the same input, but are not a plurality of inputs as required in claims 74-76. The claim construction adopted by the examiner is based entirely (and improperly) on hindsight.

Further, the central point of claim 74 is that lookup tables or parts of lookup tables are accessed in parallel by different inputs, and it is clear from the description of Fig. 4 at page 9 of Kim that in the first pipeline section 310 the upper set of bits is processed while the lower set of bits is simply stored and then used to Exclusive OR with the processed upper set to form an output of the stage 310. Then in the second stage 320 the lower set of bits is processed and the result is Exclusive ORed with the output of the first stage. So the processing of the first and second sets of bits in Kim is not in parallel as is required by claims 74-76, but instead is in series, first the upper set, then the lower set. Thus, even if lookup tables as taught by Luyster were used in Kim, the result would not be the parallel use of the two different parts of the input to access lookup tables. Instead, the upper part might be used to access a lookup table to implement the processing of the upper bits, but the lower set of bits would not be used until the upper set was done. Indeed, the second stage uses the results of processing the upper set of bits in order to generate the second stage output. This is the antithesis of “parallel” operation.

The result is that Kim et al uses two different parts of a *single* input and uses them *in series*, whereas the present invention uses *different inputs* and uses them *in parallel*. These are entirely different.

In Section II at page 7 of the Office action, the examiner responds to this distinguishing argument by asserting that the claims do not recite that the two accesses are simultaneous. While the examiner is correct that the term “simultaneously” is not used in claims 74-76, the examiner is incorrect in concluding that the concept of “simultaneous” can or should be ignored. One of ordinary skill in the art would understand that when two things are described as being done “in parallel” they are considered to be concurrent. Indeed, even the examiner concedes this, stating at page 6 of the Office action that “simultaneously is considered to be equivalent to in parallel.” The fact is that no one of skill in the art would consider an arrangement where one process is performed and then after that a second process is performed to be performing the two processes “in parallel.”

So if Kim were modified to incorporate lookup tables, it would still be the case that there would be no parallel use of plural different input signals as is required of claims 74-76.

Claims 1, 2, 5, 6, 11-13, 16, 21-28, 30, 31, 33-42, 44, 45, 47-73 and 77-79 –

The distinction of these claims over the prior art is explained in the Amendment filed November 24, 2008, from the paragraph at the bottom of page 29 and continuing on to the end of the remarks.

At page the examiner again refers to the upper and lower bits as first and second sets of bits, but the examiner has missed the point. Claim 1 requires that there be plural inputs, with each input defined by first and second sets of bits. The upper and lower sets of bits in Kim et al are different parts of the same input, and may therefore correspond to the claimed first and second sets of bits. But claim 1 recites that the method is responsive to a plurality of inputs, and for each input and *in parallel with other inputs*, there are two steps performed. First, the first set of bits of the plurality of inputs are used to access plural lookup tables with the outputs from the

lookup tables collectively forming a set of outputs. Second, the second set of bits of each input is used to select one output from the set of outputs. These two steps are performed *for each input, and in parallel with other inputs.*

If the upper and lower bits in Kim et al are considered to be the claimed first and second sets of bits, then the upper and lower bits together form an input. That is fine, but claim 1 would require that the upper bits from plural inputs access respective different lookup tables, and that the lower bits of each input signal be used to select from amongst the outputs of the plural lookup tables. This simply does not happen in Kim et al, nor would it happen if Kim et al's process were implemented using lookup tables, nor would it happen if "the output from the first bit string are used for inputs to the second string" as the examiner proposes at page 9 to adopt from 3GPP.

In Section IV at page 4, the examiner dismisses these arguments on multiple unsupportable grounds. First, the examiner argues that claim 1 does not require multiple lookup tables. The examiner is ignoring the clear language of the second subparagraph of claim 1 which reads:

looking-up one of a plurality of elements of each of *a plurality of look-up tables* using the first set of bits that define the input to obtain an output, the outputs from each of *the plurality of look-up tables* collectively comprising a set of corresponding outputs;

The examiner further argues that the Kasumi algorithm uses plural inputs, but this does not lead to the use of plural lookup tables in the particular manner recited in claim 1.

In Section V at page 5, the examiner purports to dismiss applicants arguments but the dismissal makes no sense. The examiner somehow concludes that because the Kasumi algorithm uses multiple rounds of processing the selection operation of claim 1 is inherent. There is simply no support for this. Using the output of one round as the input to the next is not what is recited in claim 1. Claim 1 describes the use of the first parts of plural inputs to access plural lookup tables to generate a plurality of lookup table outputs, and then the second part of each input being used to select one of the set of outputs. This is not the use of one stage output as an input to the next stage.

Pre-Appeal Brief Request for Review
USSN 10/762,364

The remaining independent claims all distinguish on the same basis as claim 1, and all dependent claims distinguish by virtue of their dependency. Accordingly, reversal of the examiner is requested.

Respectfully submitted,

/DJCushing/

David J. Cushing
Registration No. 28,703

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Date: August 4, 2009